UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

4832 STEWART AVE., CINCINNATI, OH 45227, AND THREE VEHICLES DESCRIBED IN ATTACHMENTS A-2, A-3, and A-4

Case No. 1:21-mj-316

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-3.

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC §§ 2252(a)(2), 2252(a)(4)(B), 2252A(a)(2)(A), 2252A(a)(5)(B)	Receipt/distribution of a visual depiction of a minor engaged in sexually explicit conduct; possession of visual depiction of minor engaged in sexually explicit conduct; receipt/distribution of child pornography; possession of child porn.

The application is based on these facts:

See Attached Affidavit (incorporated by reference).

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Kimberly.A.Wallace Digitally signed by Kimberly.A.Wallace Date: 2021.04.12 10:53:45 -04'00'

Applicant's signature

Kimberly Wallace, HSI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by FaceTime Video Conference *(specify reliable electronic means)*.

Date: **Apr 12, 2021**

Karen L. Litkovitz

Karen L. Litkovitz
United States Magistrate Judge

City and state: Cincinnati, Ohio

ATTACHMENT A-3

Property to be searched

TARGET VEHICLE 2 is a black Nissan Altima bearing Ohio license plate HVV6358 and Vehicle Identification Number 1N4AL3AP2HC284787. This search shall include all packages, bags, and hidden compartments found inside the vehicle.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. §§ 2252(a)(2), 2252(a)(4)(B), 2252A(a)(2), and 2252A(a)(5)(B) (the "Target Offenses"), those violations involving an unidentified suspect using the email address ineededdat@gmail.com and occurring after in or about January 2018, including:

   a. All visual depictions of child pornography, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, U.S.C. § 2256;

   b. Child erotica;

   c. Records and information relating to any computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

   d. Records and information relating to the production, possession, receipt, or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C § 2256, or pertaining to an interest in child pornography, whether transmitted or received;

   e. Records and information relating to the ownership or possession of the PREMISES and the TARGET VEHICLES;

f. Records and information relating to the email account ineededdat@gmail.com, and any other online accounts used in furtherance of the Target Offenses;

g. Records and information relating to online applications and cloud-storage applications that could be used to commit the Target Offenses, including usernames and passwords for those applications;

h. Records and information relating to the identity of "Esteban Underbeit" or "Esteban Beiten";

i. Computers or storage media used as a means to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"

web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF 4832 STEWART AVENUE, CINCINNATI, OHIO 45227, AND THREE VEHICLES DESCRIBED IN ATTACHMENTS A-2, A-3, AND A-4	Case No. 1:21-mj-316 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Kimberly Wallace, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION

1. This Affidavit is submitted in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the following locations for the things described in Attachment B:

a. the premises known as 4832 Stewart Avenue, Cincinnati, Ohio 45227 (the "**SUBJECT PREMISES**"), further described in Attachment A-1;

b. the gray Jeep Compass bearing Ohio license plate GLM9591 and Vehicle Identification Number 3C4NJDDBXJT129471 ("**TARGET VEHICLE 1**"), further described in Attachment A-2;

c. the black Nissan Altima bearing Ohio license plate HVV6358 and Vehicle Identification Number 1N4AL3AP2HC284787 ("**TARGET VEHICLE 2**"), further described in Attachment A-3; and

d. the gray Ford Focus bearing expired Ohio license plate FAU3519 and Vehicle Identification Number 1FADP3K22HL231771 ("**TARGET VEHICLE 3**"), further described in Attachment A-4.

2. I have been employed as a Special Agent ("SA") of the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI"), since June 2010, and am currently assigned to the HSI Resident Agent in Charge Cincinnati, Ohio office. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation, and I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

3. The statements in this Affidavit are based on information provided by other law enforcement officers and on my investigation of this matter. This Affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts in this Affidavit, I submit that there is probable cause to believe that contraband, evidence, fruits, and instrumentalities of violations 18 U.S.C. §§ 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual

depiction of a prepubescent minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (receipt or distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography involving a prepubescent minor) will be found at the **SUBJECT PREMISES**.

PERTINENT FEDERAL CRIMINAL STATUTES

5. This investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2252(a)(2) and (b)(1), prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2), prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced

using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1), prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

d. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

e. Under 18 U.S.C. § 2256, the term sexually explicit conduct includes the lascivious exhibition of the genitals or pubic area of any person.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

6. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as digital files that can be directly transferred to another device using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows a computer to connect to another computer through a telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types—to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer—can store thousands of images or videos at very high resolution. It is extremely

easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person or in an individual's vehicle. Smartphones and/or mobile phones are often carried on an individual's person. Additionally, devices and other electronic storage media can be found in an individual's vehicle.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic

communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO RECEIVE, DISTRIBUTE, AND/OR POSSESS CHILD PORNOGRAPHY

7. As a result of my training and experience in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt, distribution, and possession of child pornography.

a. These individuals may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasizing while viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. These individuals may collect sexually explicit or suggestive materials, in a variety of media, including digital and electronic media, photographs, magazines, motion pictures, video tapes, books, sliders, drawings, and/or other visual media. These individuals often use these materials for their own sexual arousal and gratification. Furthermore, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. To the extent these individuals possess and maintain "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., they almost always maintain those hard copies in the privacy and security of their home. They typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

d. Likewise, these individuals often maintain their digital or electronic collections of child sexual exploitation images in a safe, secure, and private environment, such as a computer and surrounding area, or on cellular telephones. These collections are often maintained for several years and are kept close by, usually at the individual's residence, on his or her person, or in his or her vehicles, to enable the individual to view the collection, which is valued highly. It is not uncommon for individuals involved in child pornography offenses to utilize multiple computer devices to obtain, store, or share their collections. Increasingly, individuals who view child pornography are utilizing laptop computers and other smaller devices, such as cellular telephones, iPads, and tablets to do their computing.

e. These individuals also may correspond with and/or meet others to share information and materials; are rarely able to completely destroy correspondence from other child pornography distributors/collectors; conceal correspondence as they do their sexually

explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. These individuals prefer not to be without their child sexual exploitation images for any prolonged time period. Collectors will take their collection with them if they change residences, as the collection is considered to be a prized possession. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. That said, there are individuals with a sexual interest in children who download and view digital images of child sexual exploitation, and delete them in order to avoid detection by law enforcement or other people. However, even in cases where these images are deleted, or concealed via encryption software, forensic examiners can sometimes use specialized tools to recover the deleted files or access encrypted files.

g. These individuals often use specialized software to conceal the existence of evidence and/or destroy said evidence. There are a variety of different programs that an individual can use to accomplish these objectives, many of which are free. Additionally, these individuals have been known to store child pornography in unconventional physical locations, as well as in unusual digital locations on computers and cellular phones. These files and folders, or applications, have been misnamed or renamed in an attempt to mislead investigators.

h. These individuals will often download and store images of children they know or with whom they have communicated, as well as their communications with those

children. The images may not necessarily be pornographic or obscene in nature; however, they are often used for the individuals' sexual gratification.

BACKGROUND ON CHAT APPLICATION A[1]

8. This investigation involves a secure chat platform I will call Chat Application A. Chat Application A is a communications platform based in the United States. Service is offered through a web-based application for the Windows, Linux, and iOS operating systems, along with mobile applications available for Android and iOS operating systems. Chat Application A's service includes instant messaging, voice calls, video calls, and file sharing capabilities. To create and then log into an account on Chat Application A, a user must provide a username and a unique password. Communication on Chat Application A is end-to-end encrypted and stored locally on the device used, meaning only the user can decrypt content stored on the device that is accessing Chat Application A. Communication on Chat Application A is ephemeral; Chat Application A offers various burn-on-read timer settings.

9. Based on my training and experience and from information relayed to me by other law enforcement officers, I know Chat Application A is often used for illegal activity, including exchanging and accessing child pornography, because of the high degree of anonymity that Chat Application A offers its users.

[1] Law enforcement knows the actual name of Chat Application A. However, the investigation into users of Chat Application A remains ongoing, and public disclosure of Chat Application A's actual name would potentially alert its members to the investigation, likely provoking members to notify other members of the investigation, to flee, and/or destroy evidence. Accordingly, to preserve the confidentiality and integrity of the ongoing investigation, I do not disclose the actual name and other identifying details of Chat Application A in this affidavit.

BACKGROUND OF CLOUD PLATFORM A[2]

10. This investigation also involves a secure cloud storage and file hosting service that I will call Cloud Platform A. Cloud Platform A provides communication services to a global audience and can be accessed from all major computer devices, including desktop and laptop computers, smartphones, and tablets. Cloud Platform A provides encrypted, cloud-based services that enable private, secure online storage, communication, and collaboration for businesses and individuals. A Cloud Platform A user can access several gigabytes of cloud storage free of charge for a limited time or pay for additional storage.

11. Users of Cloud Platform A can securely exchange text messages and have audio, video, or group calls with the chat function. Users of Cloud Platform A can automatically back up photos and videos from mobile devices, sync data between a computer and the secure cloud, and export secure links to files and folders, or share folders directly with other Cloud Platform A users.

12. To create and subsequently log into a Cloud Platform A account, a user must provide a valid email address, which must be verified by Cloud Platform A, and a unique password. To enter an encrypted chat room on Cloud Platform A, the user must have the link and decryption key to the chat room, which one Cloud Platform A user can share with another via hyperlink. Users within a chat room may chat and upload files that may be viewed and/or downloaded by other users in the chat room. Even before joining the encrypted chat room, an invited user has the

[2] Law enforcement knows the actual name of Cloud Platform A. However, the investigation into users of Cloud Platform A remains ongoing, and public disclosure of Cloud Platform A's actual name would potentially alert its members to the investigation, likely provoking members to notify other members of the investigation, to flee, and/or destroy evidence. Accordingly, to preserve the confidentiality and integrity of the ongoing investigation, I do not disclose the actual name and other identifying details of Cloud Platform A in this affidavit.

freedom to browse all previously uploaded conversations, image files, and video files since the inception of the chat room. Browsing the chat room content after being invited does not automatically cause the user to join the chat room; a user must manually join the chat room after being invited.

13. Cloud Platform A was launched in approximately January 2013 and is offered primarily through web-based applications. Mobile applications for Cloud Platform A are also available for Windows, Android, and iOS operating systems. Based on my training and experience, and from previous investigations I have conducted, I know Cloud Platform A is often used for illegal activity, to include the sharing and distribution of files that contain child exploitative material.

PROBABLE CAUSE

A. In July 2019, HSI agents assumed the online identity of a child-pornography target to obtain access to an encrypted chat on Chat Application A where users were exchanging child pornography.

14. In July 2019, HSI San Diego agents executed a search warrant for the residence of a target who was using Chat Application A to violate 18 U.S.C. §§ 2252 and 2252A. During the execution of the warrant, the target of the investigation consented to allow HSI San Diego agents to assume his online identity to access Chat Application A. Doing so allowed agents to access several large group chats within Chat Application A by accepting invitations from other users.

15. On or about July 12, 2020, the assumed account was added to a group chat on Chat Application A that contained many unidentified participants.

16. On or about July 14, 2020, within the aforementioned group chat on Chat Application A, a user distributed a web link invitation to an encrypted chat room within Cloud Platform A. I will call this chat room the "Encrypted Chat."

17. HSI San Diego agents accessed the invitation link to the Encrypted Chat. Prior to joining the chat room, agents recorded the contents of the Encrypted Chat dating back to its creation on May 20, 2020. The agents' review showed that there were approximately 145 registered users within the Encrypted Chat. Many users were actively involved in the distribution of child pornography dating back to on or about May 20, 2020. Files shared since the inception of the group chat were available to all chat room users regardless of the date the users joined the Encrypted Chat. Image and video files distributed within the encrypted chat room appear as thumbnail previews. Most of those thumbnail previews depict child sexual abuse material. A large portion of files distributed within the Encrypted Chat depicted at least one child engaged in sexually explicit conduct. A summary of the approximate number of child pornography files and links to file hosting websites containing child pornography (many contained gigabytes of child pornography files) distributed within the Encrypted Chat follows: 129 video files, 324 image files, and 43 cloud-storage weblinks.

18. I know from training and experience and from reviewing the content of the encrypted chat room that the primary purpose of the Encrypted Chat was to facilitate the access, receipt, and distribution of child pornography files amongst its registered users.

19. All of the 43 file-hosting weblinks noted above have since been removed by Cloud Platform A due to known and unknown parties reporting the weblinks for containing child pornography and/or for terms-of-service violations.[3]

B. An individual using the screen name "Esteban Beiten" posted, solicited, and received child pornography in the Encrypted Chat.

20. The agents' review of the Encrypted Chat showed that one user of Cloud Platform A, who uses the screen name "Esteban Beiten" and account username "ineededdat@gmail.com," joined the Encrypted Chat on or about the date it was created, on May 20, 2020. I will refer to this account as the "Esteban Beiten" account.

21. At the time "Esteban Beiten" joined the chat room, numerous image and video files depicting child pornography had previously been shared between various participants. For the reasons given above, I know that "Esteban Beiten" had the ability to view and download all files that had previously been distributed within the encrypted chat room.

22. I reviewed numerous image and video files distributed within the chat room and, based on my training and experience, I believe that many files depicted at least one child engaged in sexually explicit conduct and therefore constitute child pornography as defined in 18 U.S.C. § 2256. For example, a video file titled "cp tara ocho años.mp4", distributed on May 20, 2020, was approximately four minutes and 59 seconds in length. The video file began by depicting a nude prepubescent female wearing a mask meanwhile orally copulating the erect penis of an adult male. The video file then depicted the prepubescent female being vaginally penetrated by the erect

[3] Note that Cloud Platform A can only access the content of a cloud account when provided a complete decryption key by a reporting party. Additionally, Cloud Platform A is operated outside of the continental United States.

penis of the same adult male. Prior to the conclusion of the video file, the prepubescent female is depicted orally copulating the erect penis of the same adult male.

23. On or about May 20, 2020, "Esteban Beiten" posted an image titled "Tara 8Yr – Ass To Mouth – February 6Th 2007.wmv.jpg", which was an image sequence that appeared to match still images taken from the video described in the preceding paragraph (and, like the video itself, depicted child pornography). "Esteban Beiten" then wrote, "I need this vid."

24. Another user in the chatroom then posted the video described in paragraph 22. "Esteban Beiten" then posted two emojis of a smiling face with horns and wrote, "Thanks!"

C. The "Esteban Beiten" account on Cloud Platform A was accessed at least twice from an IP address registered to DAMON CHANCELLOR at the SUBJECT PREMISES.

25. On or about July 15, 2020, the "Esteban Beiten" account was still a member of the Encrypted Chat within Cloud Platform A. On this same date and at the request of HSI San Diego, Cloud Platform A produced subscriber information and Internet Protocol (IP) address logs associated with the "Esteban Beiten" account.

26. The subscriber information showed the following:

Account Creation Date: July 17, 2018 6:56:45 PM GMT

Registered E-Mail: ineededdat@gmail.com

Member of Encrypted Group Chats: 18

Cloud stored Files: 171

Cloud stored Folders: 2

27. As noted, Cloud Platform A also produced IP logs for the "Esteban Beiten" account. Based on my training and experience, and information relayed to me by other law enforcement officers with relevant experience, I know the following about IP logs and how to interpret them:

a. A user will open a session each time they log in to Cloud Platform A with their username (e-mail address) and password combination. One session will be allocated for each device/browser connected, and the session is only closed when the user logs out of Cloud Platform A. A user can be active as many times as they like during that session. Additionally, sessions can be long-lived; they do not correspond to a single use of Cloud Platform A, and they last from login until the user logs out, which may be hours, days, weeks, months, or even longer (if the user never logs out). The last activity time for a user is based on the most recent activity from their sessions.

b. A "creation" IP address is the IP address associated with a time when the user typed in his or her credentials (username and password) and began a session.

c. By contrast, a "first seen" or a "last seen" IP address is associated with a time during which the user was already logged in and did not need to enter his or her credentials.

28. Cloud Platform A's records showed approximately 113 unique IP addresses associated with the "Esteban Beiten" account over a period of less than two years. I queried each IP address on publicly available websites and found that these 113 IP addresses were registered to approximately 38 different companies.

29. Based on my training and experience, I know that, even if a user is using a VPN (virtual private network), which allows the user to hide his or her true residential IP address, the

various IP addresses accessed through the VPN would all come back as registered to the same VPN company. In my experience, it would be very unusual for one person to use more than 30 different VPN services in a two-year timespan. For that reason, as well as the information I describe in the next paragraph, I believe these 113 unique IP addresses and 38 companies reflect traffic being routed over the dark web rather than 113 different physical locations from which the "Esteban Beiten" account was accessed.

30. A colleague and I researched the 38 companies associated with the 113 unique IP addresses and found that most of them provided anonymous proxy servers or relay servers on the dark web. Approximately 46 of the associated IP addresses were still active dark web relays, and a sample of the remaining IP addresses showed that they were historical dark web relays (meaning that, at times in the past, they had been used as dark web relays). Based on my training and experience, I know that when a user accesses the dark web, his or her request is routed through many, sometimes even thousands, of "relay nodes" (different computers) until it finally reaches its destination; the IP address of that destination node is what appears on the IP log. Accordingly, I do not believe that any of the IP addresses associated with a dark web relay is associated with a particular physical location from which the "Esteban Beiten" account was accessed.

31. With one exception I describe below, the remaining IP addresses appeared to be registered to server or hosting companies, not to residential internet service providers (ISPs) like Comcast or AT&T. Based on my training and experience, on the fact that these remaining IP addresses are not registered to a residential ISP, and on the evidence that the other IP addresses described above were associated with dark web relays, I believe it is likely that these remaining IP

addresses also reflect traffic over the dark web rather than physical locations from which the "Esteban Beiten" account was accessed.

32. As noted above, although the vast majority of the IP addresses in the logs from Cloud Platform A appeared to reflect dark-web traffic, there were logins to the "Esteban Beiten" account on Cloud Platform A that came back to the same residential IP address. Specifically:

IP Address	Approximate Connection Date/Time	Type
75.187.80.28	July 19, 2018 12:45:53 PM GMT[4]	Creation IP
75.187.80.28:34304[5]	May 7, 2019 3:57:56 PM GMT	Last Seen IP

33. A review of open source information revealed that the above-referenced IP address is leased by Spectrum (Charter Communications, Inc.). Records from Charter showed that this IP address resolved to the same service account and service address: DAMON CHANCELLOR at the **SUBJECT PREMISES**. Contact information for the Charter account listed an email address of jedmerson@gmail.com.[6] The records showed that the lease for the account started on 02/02/2017 and ended on 08/31/2020.

[4] Note that this login occurred two days after the "Esteban Beiten" account was originally created, on July 17, 2018.

[5] The last set of digits appended to this IP address, 34304, is a "port number." A port number is "tacked on" to the end of an IP address to provide additional information about the type of communication being sent.

[6] Note that this email address incorporates the first initial and last name of JOHN EDMERSON, another individual who, as described below, lists the **SUBJECT PREMISES** as his address on his driver's license.

D. The Google account associated with the "Esteban Beiten" account on Cloud Platform A, "ineededdat@gmail.com," was also accessed from an IP address registered to CHANCELLOR at the SUBJECT PREMISES.

34. On or about February 4, 2021, Google was served with a subpoena for subscriber information for "ineededdat@gmail.com," the email address associated with the "Esteban Beiten" account on Cloud Platform A. Google responded with the following subscriber information:

Name: Esteban Underbeit
e-Mail: ineededdat@gmail.com
Created on: 2018-05-13 02:12:54 UTC
Terms of Service IP: 75.187.80.28

35. Note that the Terms of Service IP address, 75.187.80.28, is the same IP address that accessed the "Esteban Beiten" account on Cloud Platform A, as described above.

36. The most recent IP address used to log in to "ineededdat@gmail.com" was 76.181.107.133 on 10/04/2020 at 07:04:51 UTC. A review of open source information revealed that the above referenced IP address is leased by Spectrum (Charter Communications, Inc.).

37. Records from Charter showed that that the IP address was registered to DAMON CHANCELLOR at the **SUBJECT PREMISES**. Contact information for the account listed an email address of jedmerson@gmail.com (the same email address associated with the IP address described in the preceding section, which, as noted, incorporates the first initial and last name of JOHN EDMERSON; I believe based on his driver's license address that EDMERSON lives at the **SUBJECT PREMISES**). The lease for the account started on 09/16/2020 and ended on 12/23/2020.

38. Based on the evidence that the "Esteban Beiten" account on Cloud Platform A was accessed from the **SUBJECT PREMISES** at least twice and the evidence that the associated Google account—ineededdat@gmail.com—was also accessed via an IP address associated with

the **SUBJECT PREMISES**, I believe that the user of the "Esteban Beiten" account on Cloud Platform A lives at the **SUBJECT PREMISES**.

E. DAMON CHANCELLOR, PHARIN WILLIS, and JOHN EDMERSON list the SUBJECT PREMISES as their address on their driver's licenses.

39. On or about February 1, 2021, a query in the Thomson Reuters Consolidated Lead Evaluation and Reporting (CLEAR) database revealed approximately three individuals associated with the **SUBJECT PREMISES**. Specifically, the **SUBJECT PREMISES** was listed as a current address for DAMON CHANCELLOR (XX/XX/1987), PHARIN WILLIS (XX/XX/1989), and JOHN EDMERSON (XX/XX/1986).

40. On or about February 1, 2021, Ohio Law Enforcement Gateway (OHLEG) queries for the individuals referenced in Paragraph 23 revealed valid Ohio driver's licenses. All three individuals had the **SUBJECT PREMISES** listed as a residence.

F. Vehicles registered to CHANCELLOR, EDMERSON, and WILLIS were parked outside the SUBJECT PREMISES on or about April 7, 2021.

41. On or about April 7, 2021, law enforcement conducted physical surveillance at the **SUBJECT PREMISES**. Parked on Stewart Avenue in front of and near the **SUBJECT PREMISES** were three vehicles:

a. a gray Jeep Compass bearing Ohio license plate GLM9591, with VIN 3C4NJDDBXJT129471, which is registered to PHARIN WILLIS at the **SUBJECT PREMISES ("TARGET VEHICLE 1")**;

b. a black Nissan Altima bearing Ohio license plate HVV6358, with VIN 1N4AL3AP2HC284787, which is registered to DAMON CHANCELLOR at the **SUBJECT PREMISES ("TARGET VEHICLE 2")**; and

c. a gray Ford Focus bearing expired Ohio license plate FAU3519, with VIN 1FADP3K22HL231771, which was registered to JOHN EDMERSON at the **SUBJECT PREMISES ("TARGET VEHICLE 3").**

42. On or about February 12, 2021, the U.S. Postal Inspection Service verified that the **SUBJECT PREMISES** is one address; despite having two front doors, it does not have separate apartment or unit numbers.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

43. As described above and in Attachment B, this application seeks permission to search for certain records that might be found on the **SUBJECT PREMISES** and the **TARGET VEHICLES**, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of computers and electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

44. *Probable cause.* Given the information set forth above, I submit that if a computer or electronic storage medium is found on the **SUBJECT PREMISES** or in the **TARGET VEHICLES**, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools.

This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

45. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only computer files and electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There

is probable cause to believe that this forensic electronic evidence will be on any computer or electronic storage medium in the **SUBJECT PREMISES** or in the **TARGET VEHICLES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online usernames, nicknames, and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or

storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate

the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for

committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

46. *Necessity of seizing or copying entire computers or storage media.* Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed

or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

47. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

48. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying computers and electronic storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to

computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

49. Because it appears that several people share the **SUBJECT PREMISES** as a residence, it is possible that the **SUBJECT PREMISES** will contain computers or electronic storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or electronic storage media, the warrant applied for would permit the seizure and review of those items as well.

SEARCH METHODOLOGY TO BE EMPLOYED

50. All computers, other computer hardware, computer software, and any form of electronic storage media that could contain evidence described in this warrant may be seized for an off-site search for evidence that is described in the attachments of this warrant. It is anticipated that mirror copies or images of such evidence will be made if the failure to do so could otherwise potentially alter the original evidence.

51. The search procedure of electronic data contained in computers, other computer hardware, computer software, and/or electronic storage media may include the following techniques (the following is a non-exhaustive list, as other search procedures may be used):

a. On-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;

b. On-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;

c. Examination of all of the data contained in such computers, other computer hardware, computer software, or electronic storage media to view the data and determine whether that data falls within the items to be seized as set forth herein;

d. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

e. Surveying various file directories and the individual files they contain;

f. Opening files in order to determine their contents;

g. Scanning storage areas;

h. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

i. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

52. Contextual information necessary to understand the evidence, to identify the user/possessor of the child pornography, and to establish admissibility of the evidence in subsequent legal proceedings will also be sought by investigative agents.

53. Because it is expected that the computers, other computer hardware, computer software, and any form of electronic storage media may constitute (1) instrumentalities of the offense, (2) fruit of criminal activity, (3) contraband, or (4) evidence otherwise unlawfully possessed, it is anticipated that such evidence will not be returned to the owner and that it will be either forfeited or ultimately destroyed in accordance with the law at the conclusion of the case.

a. Because of the large storage capacity as well as the possibility of hidden data within the computers, other computer hardware, and any form of electronic storage media, it is anticipated that there will be no way to ensure that contraband-free evidence could be returned to the user/possessor of the computer, other computer hardware, or any form of electronic storage media, without first wiping such evidence clean. Wiping the original evidence clean would mean that the original evidence would be destroyed and thus, would be detrimental to the investigation and prosecution of this case.

b. Further, because investigators cannot anticipate all potential defenses to the offenses in this Affidavit, and as such, cannot anticipate the significance of the evidence that has been lawfully seized pursuant to this warrant, it is requested that all seized evidence be retained by law enforcement until the conclusion of legal proceedings or until other order of the court.

c. If after careful inspection investigators determine that such computers, other computer hardware, computer software, and electronic storage media do not contain or

constitute (1) instrumentalities of the offense, (2) fruit of criminal activity, (3) contraband, (4) evidence otherwise unlawfully possessed, or (5) evidence of the person who committed the offense and under what circumstances the offense was committed, then such items seized will be returned.

CONCLUSION

54. Based on the foregoing, there is probable cause to believe that contraband, property, evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a prepubescent minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (receipt or distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography involving a prepubescent minor), as described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

//

//

//

//

//

//

55. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, each of the "return" inventories will contain a list of only the tangible items recovered from the **SUBJECT PREMISES** and the **TARGET VEHICLES**. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Kimberly.A.Wallace Digitally signed by Kimberly.A.Wallace Date: 2021.04.12 10:54:22 -04'(

Kimberly Wallace
Special Agent
Homeland Security Investigations

Sworn and subscribed before me via FaceTime videoconference this 12th day of April, 2021.

Karen L. Litkovitz
United States Magistrate Judge

ATTACHMENT A-3

Property to be searched

TARGET VEHICLE 2 is a black Nissan Altima bearing Ohio license plate HVV6358 and Vehicle Identification Number 1N4AL3AP2HC284787. This search shall include all packages, bags, and hidden compartments found inside the vehicle.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. §§ 2252(a)(2), 2252(a)(4)(B), 2252A(a)(2), and 2252A(a)(5)(B) (the "Target Offenses"), those violations involving an unidentified suspect using the email address ineededdat@gmail.com and occurring after in or about January 2018, including:

   a. All visual depictions of child pornography, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, U.S.C. § 2256;

   b. Child erotica;

   c. Records and information relating to any computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

   d. Records and information relating to the production, possession, receipt, or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C § 2256, or pertaining to an interest in child pornography, whether transmitted or received;

   e. Records and information relating to the ownership or possession of the PREMISES and the TARGET VEHICLES;

f. Records and information relating to the email account ineededdat@gmail.com, and any other online accounts used in furtherance of the Target Offenses;

g. Records and information relating to online applications and cloud-storage applications that could be used to commit the Target Offenses, including usernames and passwords for those applications;

h. Records and information relating to the identity of "Esteban Underbeit" or "Esteban Beiten";

i. Computers or storage media used as a means to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"

web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.